AMENDMENT TO THE SPECIFICATION

Please amend the specification as follows.

Please replace paragraph [63] with the following:

--By way of example, a path selection rule may select the path based on any of the following path information in which IP packets match the rule: a primary path, a secondary path, and a tertiary path. The primary path ~~is~~ may be specified in any path selection rule. The secondary path is used only when the primary path has failed. If no secondary path is specified, any IP packets that match the rule can be discarded when the primary path fails. The tertiary path is specified only if a secondary path is specified. The tertiary path is selected if both the primary and secondary paths have failed. If no tertiary path is specified, any IP packets that match the rule can be discarded when both the primary and secondary paths fail. Path selection may be generalized such that the path selection rule can select up to N paths where the Nth path is used only if the (N-1)th path fails. The example above where N=3 is merely illustrative, although N is typically a fairly small number.--

Please replace paragraph [77] with the following:

--When a Connection Request message is received from a peer TSK (step 403), the TCP Spoofing Kernel 280 allocates a CCB for the connection and then stores all of the relevant information from the CR message in the CCB. TSK 280 of PEP end point 404 then uses this information to generate a TCP <SYN> segment, as in step 415, to send to the remote host 406. The MSS in the <SYN> segment is set to the value received from the TSK peer of PEP end point 404. When the remote host responds with a TCP <SYN,ACK> segment (step 417), TSK 280 of PEP end point ~~402~~ 404 sends a Connection Established message to its TSK peer of the ~~remote~~ PEP end point ~~404~~ 402 (step 419), including in the CE message the MSS that is sent by the local host in the <SYN,ACK> segment. TSK 280 of PEP end point ~~402~~ 404 also responds, as in step 421, with a TCP <ACK> segment to complete the local three-way handshake. The peer TSK of PEP end point 404 then forwards the data that is received from TSK 280 to the host, per step 423. Concurrently, in step 425, the remote host 406 sends data to the peer TSK of PEP end point 404, which acknowledges receipt of the data by issuing an <ACK> segment to the ~~remote PEP~~

~~end point 404~~ host 406, per step 427. Simultaneously with the acknowledgement, the data is sent to TSK 280 of PEP end point 402 (step 429).--

Please replace paragraph [85] with the following:

-- For WAN-to-local traffic (i.e., downstream direction), the remote PEP end point 503 receives IP packets from its WAN interface 230 (Figure 2). IP packets that are not addressed to the end point 503 are simply forwarded (as appropriate) to the local interface 220 (Figure 2). IP packets addressed to the end point 503, which have a next protocol header type of "PEP Backbone Protocol (PBP)" are forwarded to the backbone protocol kernel 503c. The backbone protocol kernel 503c extracts the TCP data and forwards it to the TCP spoofing kernel 503b for transmission on the appropriate spoofed TCP connection. In addition to carrying TCP data, the backbone protocol connection is used by the TCP spoofing kernel 501b to send control information to its peer TCP spoofing kernel 503b in the remote PEP end point 503 to coordinate connection establishment and connection termination.--

Please replace paragraph [90] with the following:

-- Figure 6 illustrates the flow of IP packets through a PEP end point, according to an embodiment of the present invention. When IP packets are received at the local LAN interface 220, the PEP end point 210 determines (as shown by decision point A), whether the packets are destined for a host that is locally situated; if so, the IP packets are forwarded to the proper local LAN interface 220. If the IP packets are destined for a remote host, then the PEP end point 210 decides, per decision point B, whether the traffic is a TCP segment. If the PEP end point 210 determines that in fact the packets are TCP segments, then the TSK 280 determines whether the TCP connection should be spoofed (decision point C). However, if the PEP end point 210 determines that the packets are not TCP segments, then the BPK 282 processes the traffic, along with the PK 284 and the PSK 286 for eventual transmission out to the WAN. It should be noted that the BPK 282 does not process unspoofed IP packets; i.e., the packets flow directly to PK 284. As seen in Figure 6, traffic that is received from the WAN interface 230 is examined to determine whether the traffic is a proper PBP segment (decision point D) for the particular PEP end point 210; if the determination is in the affirmative, then the packets are sent to the BPK 282 and then the TSK 280.--

Please replace paragraph [95] with the following:

-- Figure 8 shows the interfaces of the PEP end point implemented as an IP gateway, according to one embodiment of the present invention. By way of example, an IP Gateway 801 has a single local LAN interface, which is an enterprise interface ~~803~~ <u>801</u>. The IP Gateway 803 employs two WAN interfaces 805 for sending and receiving IP packets to and from remote site PEP End Points: a backbone LAN interface and a wide area access (WAA) LAN interface. --

Please replace paragraph [99] with the following:

-- Figure 10 shows a Multimedia VSAT implementation of the PEP end point, according to one embodiment of the present invention. A Multimedia VSAT 1001, in an exemplary embodiment, has two local LAN interfaces 1003. Support for one or more local PPP serial port interfaces may be utilized. The Multimedia VSAT 1001 has two WAN interfaces 1005 for sending IP packets to hub site PEP End Points: a VSAT inroute and one of its LAN interfaces. The Multimedia VSAT 1001 thus has three interfaces for receiving IP packets from hub site PEP End Points, the VSAT outroute and both of its LAN interfaces 1003. A Multimedia VSAT ~~1003~~ <u>1001</u> may support uses of both of its LAN interfaces ~~1003~~ <u>1001</u> at the same time for sending and receiving IP packets to and from hub site PEP End Points. The Multimedia VSAT 1003 further supports the use of a VADB serial port interface for sending and receiving IP packets to and from the hub site PEP End Points. --

Please replace paragraph [101] with the following:

-- Figure 12 shows a diagram of an exemplary network management system (NMS) for PEP end points, according to an embodiment of the present invention. As shown, a communication system 1200 includes a hub (or local) site PEP end point 1201 that contains a <u>Simple Network Management Protocol</u> <u>(SNMP)</u> agent 1203. As previously discussed, hub (or local) site PEP end point 1201 may communicate via a WAN 1205 to a remote PEP end point 1207, which similarly provides a SNMP agent 1209. In an exemplary embodiment, hub (or local) site PEP end point 1201 connects to a LAN 1211. A network management system 1213 receives data from SNMP agents 1203 and 1209. The NMS 1213 maintains a database 1215 that stores an event log to assist in debugging of either of the hub (or local) site PEP end

point 1201 or the remote PEP end point. Also, the NMS 1213 includes an operator console 1217 to support logging in of events.--

Please replace paragraph [106] with the following:

-- As seen in Figure 12, each PEP End Point platform 1201 and 1207 includes an SNMP Agent 1203 and 1209, respectively, for processing get and set access to the SNMP Management Information Base (MIB) variables that are defined for the particular platform 1201 and 1207. To support access to PEP specific MIB variables, each of the SNMP Agents 1203 and 1209 accesses information kept in corresponding platform environments and PEP kernels. Access to PEP kernel information is provided via the platform environment, which represents the PEP feature to the rest of the platform software (i.e., the rest of the platform software should not even be aware that the PEP kernels exist). And, the mechanism used to access MIB information may not be consistent across all of the PEP End Point platforms; for example, a shared memory mechanism may be used in the IP Gateway, whereas a procedural interface mechanism may be used in a Multimedia VSAT. Therefore, platform specific support may be required (and providing platform specific support is one of the functions of the platform environment). --

Please replace paragraph [117] with the following:

-- The NMS 1213 implements extensive cross–checking for profile and PEP End Point creation and modification scenarios to ensure that a PEP End Point 1201, 1207 is never configured with conflicting connectivity and selective TCP spoofing criteria. In particular, the NMS 1213 performs cross checking for most scenarios; for the other scenarios, a PEP End Point 1201, 1207 may post an event to alert the operator if a TCP connection gets mapped to a non–existent backbone connection. For example, when a connectivity profile is created or modified, the profile is cross–checked against the TCP spoofing selection profile and TCP spoofing parameter profiles that are used by the IP Gateway 1201 which the connectivity profile references. When a remote site PEP End Point 1207 is created or the connectivity profile and/or TCP spoofing selection profile being used by an existing remote site PEP End Point 1207 is changed, the connectivity profile associated with the PEP end point 1207 is cross–checked against the TCP spoofing selection profile and TCP spoofing parameter profiles it is using. When the TCP spoofing selection profile being used by a hub (or local) site PEP End Point 1201 is changed, the new TCP spoofing selection

profile is ~~be~~ cross–checked against all connectivity profiles which reference the PEP End Point. Also, when the NMS 1213 does a cross–check, if an inconsistency is found, the NMS 1213 may not automatically reject the create or modify operation. Instead, the NMS I213 may simply provide a warning to the operator and prompt the operator to determine whether the create or modify operation should proceed anyway. Taking this approach eliminates any "chicken and egg" issues which might otherwise have to be addressed regarding the order of changing parameters. And, the approach advantageously provides flexibility if it turns out that intentionally having mismatched parameters is useful. For example, it might be useful to remove a backbone connection from a connectivity profile as an easy way to compare spoofed versus unspoofed performance. And, removing the backbone connection may often be easier than modifying the applicable selective TCP spoofing rules. --

Please replace paragraph [136] with the following:

-- Computer system 1401 also includes one or more communication interfaces 1419 coupled to bus 1403. Communication interfaces 1419 provide a two-way data communication coupling to network links 1421 and 1422, which are connected to a local area network ~~14~~(LAN) 1423 and a wide area network (WAN) 1424, respectively. The WAN 1424, according to one embodiment of the present invention, may be a satellite network. For example, communication interface 1419 may be a network interface card to attach to any packet switched LAN. As another example, communication interface 1419 may be an asymmetrical digital subscriber line (ADSL) card, an integrated services digital network (ISDN) card, a cable modem, or a modem to provide a data communication connection to a corresponding type of telephone line. Wireless links may also be implemented. In any such implementation, communication interface 1419 sends and receives electrical, electromagnetic or optical signals that carry digital data streams representing various types of information. --

Please replace paragraph [137] with the following:

[03]Network link 1421 typically provides data communication through one or more networks to other data devices. For example, network link 1421 may provide a connection through local area network 1423 to a host computer 1425 or to data equipment operated by an Internet Service Provider (ISP) 1427. ISP 1427 in turn provides data communication services through the Internet 505. In addition, LAN 1423 is linked to

an intranet 1429. The intranet 1429, LAN 1423 and Internet ~~505~~ all use electrical, electromagnetic or optical signals that carry digital data streams. The signals through the various networks and the signals on network link 1421 and through communication interface 1419, which carry the digital data to and from computer system 1401, are exemplary forms of carrier waves transporting the information.

Please replace paragraph [138] with the following:

-- Computer system 1401 can send messages and receive data, including program code, through the network(s), network link 1421 and communication interface 1419. In the Internet example, a server 1431 might transmit a requested code for an application program through Internet ~~505~~, ISP 1427, LAN 1423 and communication interface 1419. The received code may be executed by processor 1405 as it is received, and/or stored in storage device 1411, or other non-volatile storage for later execution. In this manner, computer system 1401 may obtain application code in the form of a carrier wave. Computer system 1401 can transmit notifications and receive data, including program code, through the network(s), network link 1421 and communication interface 1419. --